29/07/2021

Basiq.io
21C Whistler St,
Manly NSW 2095

Via Email: data@treasury.gov.au

Basiq welcomes the opportunity to respond to the exposure draft of the Competition and Consumer (Consumer Data Right) Amendment Rules (No. 1) 2021. Basiq is an Accredited Data Recipient delivering Consumer Data Right solutions to Data Holders, ADRs and FinTechs providing innovative solutions.

Basiq welcomes the move to enable access to CDR data without the prerequisite of an organisation becoming a fully accredited ADR. Our customer base covers a wide spectrum from large banks and financial institutions right down to the FinTech innovators of the future. Our focus is on enabling our customers to provide services to consumers.

In much of this response, Basiq intends to champion the voice of this smaller end of town as we feel the current implementation of CDR accreditation is not addressing the issue of the high cost and effort entry criteria to gain access to CDR Data. Having a view on CDR from a consumer perspective is paramount but seeing the rules from the perspective of innovators providing services to those consumers by leveraging CDR data is equally important. If this perspective is not supported, the high cost to innovate will be inhibitory.

Basiq also feels the other end of the spectrum of access points to CDR data is providing a very free and ungoverned route to either a subset of persons (Truster Advisors) or a subset of CDR data (CDR Insights). Basiq supports this approach but believes catchment should be widened to further support Fintech innovators.

Being aware that one of the primary drivers for CDR has been based on a particular use-case of driving better value products and services for consumers in the banking and energy sectors by spurring increased competition. Our primary recommendation in this document is a simplification of the amendment that will provide an access path to innovators whilst maintaining the right level of governance and liabilities on the correct parties.

Review of Proposed Accreditation Options

Overview

Overall the draft legislation put forward as part of this review was very welcome. The recommendations included many different accreditation models which spanned an array of use cases and requirements. They also addressed important topics concerning liability, collection, sharing and usage of data and discussed methods of accreditation and requirements to maintain the register of participants within the ecosystem.

Reviewing the differences in the proposed models, we found that the levels of responsibility, liability and data accessibility varied greatly. We saw two ends of a spectrum:

1. On one end the introduction of a sponsorship model seemed to slightly reduce the barrier of accreditation with an increased responsibility for the ADR that wants to avail itself of this model.

2. At the other end, a range of organisations with access to CDR data and no legal requirements regarding such access under the CDR regime.

The table below identifies the various methods that were recommended within the paper. The table highlights all the participants, and identifies the various liabilities, and features of what they can / cannot do.

Party	Liability	Data Collection	CDR Data Access	Data Usage
ADR (Full)	Self	✓	✓	✓
ADR (Sponsor)	Self	✓	✓	✓
Unaccredited OSP	ADR (Full)	✓	✓	✕
Affiliate of Sponsor	Self	✕	✓	✓
CDR Representative	ADR (Principal)	✕	✓	✓
Trusted Advisers	Self	✕	✓	✓

Definitions:

- **Party** - Entity identified within the recommendations.
- **Liability** - Identifies the party responsible for the liability of CDR data.
- **Data Collection** - Identifies if the party is able to collect CDR data (i.e. call the API services directly from data holders).
- **CDR Data Access** - Identifies whether the party is able to access the data i.e. does the data pass through the parties systems (software products).
- **Data Usage** - Identifies whether the party has the right to use the CDR data for intended purposes.

In review of these recommendations, what was apparent was that business structures, and usage of CDR data along with accreditation rules are incredibly complex to balance. This created a lot of internal debate within our organisation, and challenged us to think about what would possibly be a more ideal approach. Within our response below, we have tried to balance the protection of the consumer's data, ensuring that there is an appropriate governance structure to support the ecosystem and a system by which innovators can use CDR data to deliver valuable services to consumers.

Sponsorship Affiliate accreditation

Sponsorship is onerous on smaller companies

Basiq can see that the sponsorship model can be valuable for groups of companies where legal entities have different needs or tasks regarding CDR data but draw on the same IT

infrastructure and environment. However, Basiq does not believe that the sponsorship model lowers the barrier to entry sufficiently for FinTechs looking to work with an ADR that is an independent third party organisation. It would appear that in this instance there is a shift of some of the effort and cost from the affiliate to the sponsor (as compared to both being fully accredited) as the affiliate is not required to submit an assurance report but the sponsor will need to have a third party management program.

Basiq believes that the benefit of this model in the space of innovators and smaller organisations may still be quite limited. A principles based approach regarding responsibilities and liability for the affiliate is also something large organisations will be more accustomed to and comfortable with - whilst the smaller ones will struggle.

Sponsorship is costly for most organisations

We believe that under a sponsor model, sponsors should not be required to provide an annual review and assurance activities on the design and operating effectiveness of information security controls of the affiliate. A Sponsor may not have the necessary audit capabilities (typically carried out by companies specialising in this service) and would therefore incur cost to engage an external auditor to provide assistance.

Sponsorship should be a binding and exclusive relationship

The costs to the sponsor have the ability to be quite large, due to the following requirements: (1) Vetting/due diligence of new customers; (2) Initial training and ongoing training requirements; (3) Ongoing monitoring and auditing. However, within the proposed recommendation there is no mention of exclusive or a binding relationship to protect the sponsor under this mode. It is therefore hard to justify the costs as a sponsor to assist an affiliate to receive accreditation if that organisation is subsequently able to receive data from other ADRs.

The shared liability with sponsor model is unclear

Basiq recommends that any breach from the ADR or if the ADR has passed data that breaks a consumer consent rule or ADR has passed too much data to an Affiliate with regard to the data minimisation principle then the Sponsor is responsible. Any breach or misuse of Data on the Affiliate should mean they are solely responsible.

Principal CDR Representative model

The CDR Representative should be responsible for data they hold

The ADR is fully liable for the representative under this model. Again, this could be a feasible approach for group entities. However, assuming full liability for an independent third party may pose a prohibitive risk to an ADR.

It implies that the ADR by contractual arrangement, training, monitoring, and auditing has to ensure full compliance by a third party FinTech of the requirements of the CDR regime. Passing on liability that may be incurred by the ADR due to actions of the FinTech is also only possible to the extent the FinTech is an organisation of sufficient size and standing to cover the liability regime imposed by the CDR legislation. Again, the market of smaller organisations and innovators appears at a disadvantage.

Trusted Advisor model

Trusted Advisors may not have CDR level data security and governance practices

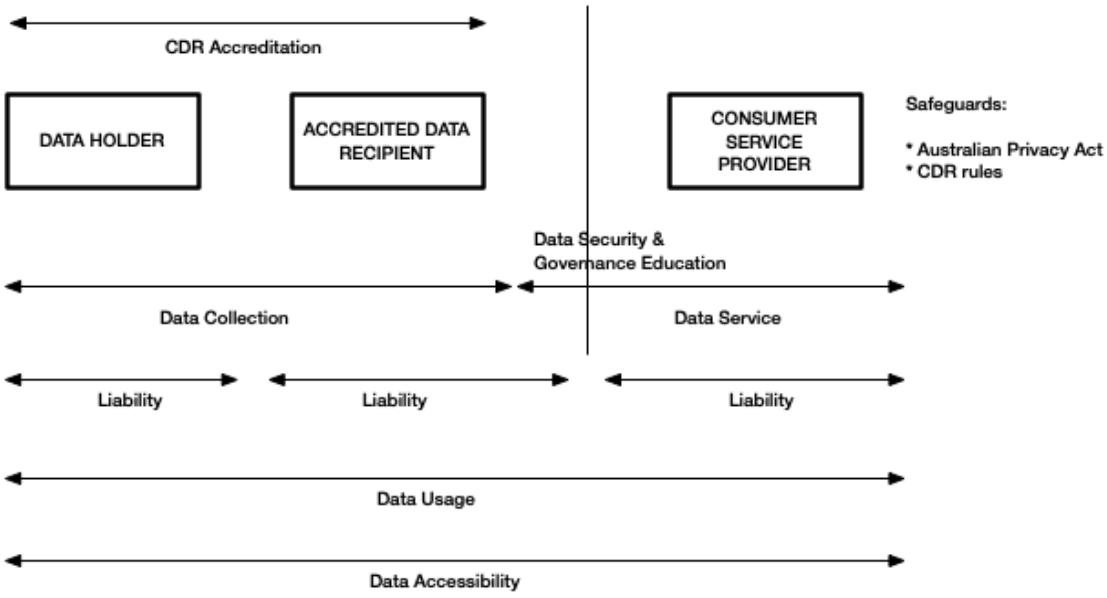
Trusted Advisors have licence accreditations outside of the CDR regime that govern and regulate the service they provide to Consumers. These Licences are not guaranteed to cover data security and governance requirements to a CDR level. Providing CDR data to these persons without a base level of education and assistance with regard to CDR defined data security and governance is a risk.

Our Recommendation

Recommended Approach

Considering the options that have been presented, we believe that a more simplified approach which is principle-based would help reduce the complexity of accreditation, increase adoption and participation within the CDR ecosystem. Basiq proposes that a potential solution to fulfilling these requirements could work as follows:

- CDR data should be able to shared with unaccredited parties
- Accessing CDR Data from Data Holders should be regulated
- ADRs responsibilities should be increased
- Each party should be liable for themselves



CDR data should be sharable with unaccredited parties

From the recommendations put forward on the various accreditation levels there was overall consistency in the willingness to share data with unaccredited parties e.g. trusted advisers, insight data etc. We suggest that this be extended to every registered business within Australia that operates within the Australian Privacy Act.

Majority of these companies already handle customers data and in some cases data that could be deemed even more sensitive than CDR data e.g. some businesses require customers to supply their passport or driver's licence as proof of identity or may hold customers medical data. In most instances, these businesses may also require customers to supply their personal identifiable information which is typical when completing online forms or registering for a new application.

If these businesses already deal with sensitive data, and are not prohibited from asking consumers for such data and are able to operate outside of an accreditation model, then ultimately we see no reason why CDR data should be any different. Enabling the consented sharing of CDR data should be something that is not prohibited through an accreditation process.

We do however recommend that wherever the data travels (as per consumers consent) that the consent / rules that were granted are respected by each party that receives the data. It also goes without saying that the data may only be shared with whomever the consumer consented to and no other party.

Accessing CDR Data from Data Holders should be regulated

Organisation that require direct access and communication with Data Holders should continue to be regulated as per current requirements. These should not be eased, as the technical and data governance responsibilities are quite high.

ADRs responsibilities should be increased

The ADR should be responsible for a stipulated level of education* around Data Security and Governance to ensure any organisation that acquired CDR data via their platform is versed on best practices and principles of data protection.

Each party should be liable for themselves

We believe that each party should be ultimately responsible / liable for their own actions and handling of CDR data. As an additional safeguard, the Privacy Act could be extended to apply not only to ADRs but to all recipients of CDR data to provide for a uniform regime including smaller entities for PII data.

Data Holder	Liable for the provision of consented data and the management of that consent.
ADR	Liable for the collection, storage and use of consented data and the management of that consent.
CSPs	Liable for the storage and use of consented data and the management of that consent. i.e. become directly subject to CDR rules regarding CDR consumer consent and certain privacy safeguards (similar to the required contractual regime under the proposed principal / representative model). We recommend that any CSP receiving PII data contained within CDR data becomes liable under the Privacy Act 1988 (currently a $3m turnover threshold) which already regulates the handling of personal information about individuals, including: ○ Collection ○ Consent ○ Use ○ Storage ○ Disclosure

Summary

Basiq believe our recommended CSP model will greatly assist in empowering several of the Government's intentions in implementing CDR to:

1. Facilitate greater participation in the CDR regime by participants and consumers
2. Promote innovation of CDR offerings including intermediary services
3. Enable services to be more effectively and efficiently provided to consumers

Basiq hopes that the ACCC finds this document informative and our recommendations a useful input for consideration. We believe the ACCC, Treasury and the DSB are doing a fantastic job bringing structure, consistency and governance to a very complicated space and we wholeheartedly thank you for the opportunity to provide our feedback and recommendation that will hopefully help facilitate a path to greater innovation and consumer benefit from the Consumer Data Rights.